BitLocker Unlock Policies

Serever 2012

Network Unlock sequence

- Install the WDS Server role
- Confirm the WDS Service is running
- Install the Network Unlock feature
- Create the Network Unlock certificate
- Deploy the private key and certificate to the WDS server
- Configure Group Policy settings for Network Unlock

Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption Network Unlock Certificate

Network Unlock Group Policy settings

Within Group Policy Management Console, navigate to the following location: **Computer configuration\Policies\Windows Settings\Security Settings\Public Key Policies\BitLocker Drive Encryption Network Unlock Certificate**

Right-click the folder and choose **Add Network Unlock Certificate**

Follow the wizard steps and import the .cer file that was copied earlier.

An additional recommendation is for enterprises to use TPM+PIN protectors for an extra level of security. To require TPM+PIN protectors in an environment, do the following:

- Open Group Policy Management Console (gpmc.msc)
- Enable the policy **Require additional authentication at startup** and select the **Require startup PIN with TPM** option

Turn on BitLocker with TPM+PIN protectors on all domain-joined computers


Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities